EXHIBIT FF

CISA CYBERSECURITY ADVISORY COMMITTEE

KICKOFF MEETING DETAILS, MEMBER INFORMATION, AND COMMITTEE BACKGROUND MATERIALS

TABLE OF CONTENTS

CISA CYBERSECURITY ADVISORY COMMITTEE

MITRE 1 Building
7525 Colshire Drive
McLean, VA 22102

ADMINISTRATIVE SESSION

MITRE 1 Building, Room 1H300

9:00 a.m. **Welcoming Remarks**
- The Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA)

9:15 a.m. **Administrative Brief**
- Federal Advisory Committee Act Overview: Alaina Clark, Assistant Director for Stakeholder Engagement

9:30 a.m. **Internal Committee Activity**
- Swearing-in of Committee members
- Committee Chair and Vice Chair nominations and voting

CLOSED SESSION

MITRE 1 Building, Room TBP

10:30 a.m. **Threat Briefing and Discussion**
- Mr. Christopher Porter, National Intelligence Officer for Cyber, Office of the Director of National Intelligence
- Mr. Rob Joyce, Director of Cybersecurity, National Security Agency
- Director Easterly
- Committee members

12:00 p.m. **Lunch**

OPEN SESSION

MITRE 1 Building, Room 1H300

1:00 p.m. **Call to Order and Opening Remarks**
- Ms. Megan Tsuyi, CISA Cybersecurity Advisory Committee Designated Federal Officer
- Director Easterly
- Committee Chair
- Committee Vice Chair

1:10 p.m. **Keynote Address**
- The Honorable Alejandro Mayorkas, Secretary of Homeland Security

1:20 p.m. **Fortifying the Nation's Cybersecurity Posture**
- The Honorable Chris Inglis, National Cyber Director

1:30 p.m. **CISA Overview**
- CISA Overview: Director Easterly
- Cybersecurity Division Mission Brief: Mr. Eric Goldstein, Executive Assistant Director for Cybersecurity
- Systemic Risk & National Critical Functions: Mr. Robert Kolasky, Assistant Director, National Risk Management Center
- Cyber Talent Management System: Mr. Nitin Natarajan, Deputy Director

2:20 p.m. **CISA's Big Challenges & Issue Tasking**
- Director Easterly
- Committee members

3:10 p.m. **Public Comment Period**

3:20 p.m. **Closing Remarks and Adjournment**
- Director Easterly
- Committee Chair
- Committee Vice Chair

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBERS

Current as of December 10, 2021

Chair

TBD

Vice Chair

TBD

Mr. Steve Adler
Mayor
Austin, Texas

Ms. Marene Allison
Chief Information Security Officer
Johnson & Johnson

Ms. Lori Beer
Chief Information Officer
JPMorgan Chase

Mr. Robert Chesney
James A. Baker III Chair in the Rule of Law and World Affairs
University of Texas School of Law

Mr. Thomas Fanning
Chairman, President, and CEO
Southern Company

Ms. Vijaya Gadde
Legal, Public Policy, and Trust and Safety Lead
Twitter

Dr. Patrick Gallagher
Chancellor
University of Pittsburgh

Mr. Ronald James Green Jr.
Executive Vice President and Chief Security Officer
Mastercard

Ms. Niloofar Razi Howe
Board Member
Tenable

Mr. Kevin Mandia
Chief Executive Officer
Mandiant, Inc.

Mr. Jeff Moss
President
DEF CON Communications

Ms. Nuala O'Connor
Senior Vice President & Chief Counsel, Digital Citizenship
Walmart

Ms. Nicole Perlroth
Author and Journalist

Mr. Matthew Prince
Chief Executive Officer
Cloudflare

Mr. Ted Schlein
General Partner
Kleiner Perkins Caufield & Byers

Mr. Stephen Schmidt
Chief Information Security Officer
Amazon Web Services

Ms. Suzanne Spaulding
Senior Advisor for Homeland Security
Center for Strategic and International Studies

Mr. Alex Stamos
Partner
Krebs Stamos Group

Dr. Kate Starbird
Associate Professor, Human Centered Design & Engineering
University of Washington

Mr. George Stathakopoulos
Vice President of Corporate Information Security
Apple

Ms. Alicia Tate-Nadeau
Director
Illinois Emergency Management Agency

Ms. Nicole Wong
Principal
NWong Strategies Group

Mr. Chris Young
Executive Vice President of Business Development, Strategy, and Ventures
Microsoft

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Mr. Steve Adler

Mayor
Austin, Texas

Mr. Steve Adler is Austin's 52nd Mayor, having won re-election in 2018 by 40 points in a field of 8 candidates. His top priorities include mobility, affordability, and equity for all Austinites. Mayor Adler is a Trustee of the United States Conference of Mayors, Past Chair of the Capital Area Metropolitan Planning Organization (CAMPO) policy board, and Vice President of the National Council of Democratic Mayors. While he's been in office the City of Austin passed the largest mobility and affordable housing bonds in its history. The city raised its minimum city wage to $15 per hour, passed city-wide sick leave and second chance hiring protections. Still working on the homelessness challenge, the city has become one of a limited number of cities to achieve effective net zero veteran homelessness. The city has become a world leader on climate change action. Mayor Adler has received broad recognition for innovative leadership. Foreign Policy named him a Global reThinker and Living Cities included Mayor Adler on its list of 25 Disruptive Leaders (along with Facebook's Mark Zuckerberg and author Ta-Nehisi Coates) to mark that organization's 25th anniversary.

Ms. Marene Allison

Chief Information Security Officer
Johnson & Johnson

Ms. Marene Allison currently serves as the Chief Information Security Officer for Johnson & Johnson, a position she has held since 2010. In this role, she is responsible for information technology and data security for one of the world's largest healthcare companies. Ms. Allison created a world class product security capability to protect a supply chain with over 120 manufacturing sites and 200 third party distributors. Prior to joining Johnson & Johnson, Ms. Allison served as Vice President and Global Security and Chief Security Officer for Medco. There, she was responsible for developing and implementing security strategy and maintaining IT and physical security for over 145 facilities. Ms. Allison also previously served as Director of Corporate Security for Avaya where she was responsible for the developing and directing the security strategy and managing threats to company's infrastructure and its revenue generating business units.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Ms. Lori Beer

Chief Information Officer
JPMorgan Chase

Ms. Lori Beer is the Global Chief Information Officer of JPMorgan Chase & Co. and a member of the company's Operating Committee, responsible for the firm's technology systems and infrastructure worldwide. In this role, she manages a budget of more than $12 billion and over 53,000 technologists supporting JPMorgan Chase's retail, wholesale and asset and wealth management businesses. She also serves as the co-sponsor of the firm's Access Ability Business Resource Group. Ms. Beer joined the firm in 2014 and was most recently the Chief Information Officer for the Corporate & Investment Bank . Prior to joining JPMorgan, she was Executive Vice President of Specialty Businesses and Information Technology for WellPoint, Inc., responsible for a $10 billion business unit which included WellPoint's Specialty Products. Ms. Beer serves as a Trustee of the University of Cincinnati Foundation Board and a member of the Teach for America New York Advisory Board. She has endowed scholarships at the University of Cincinnati and University of Dayton to help increase diversity in STEM careers.

Mr. Robert Chesney

James A. Baker III Chair in the Rule of Law and World Affairs; and
Associate Dean for Academic Affairs
University of Texas School of Law

Mr. Robert Chesney currently holds the James Baker Chair and also serves as the Associate Dean for Academic Affairs at the University of Texas School of Law. In addition, he is the Director of the Robert S. Strauss Center for International Security and Law, a University-wide research unit that includes a focus on cybersecurity. Professor Chesney's scholarship focuses on an array of U.S. national security policies and institutions, including among other things those relating to cybersecurity and other cyber domain activities. Professor Chesney is a co-founder and contributor to www.lawfareblog.com, the leading online source for analysis, commentary, and news relating to law and national security. In the past he has served the Intelligence Community in an advisory capacity as an associate member of the Intelligence Science Board and as a member of the Advanced Technology Board. He is a member of the American Law Institute.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Mr. Thomas A. Fanning

Chair, President, and Chief Executive Officer (CEO)
Southern Company

Mr. Thomas A. Fanning is Chair, President, and CEO of Southern Company, the second largest utility company in the United States. Mr. Fanning has worked for Southern Company for more than 40 years and has held 15 different positions in eight different business units, including numerous officer positions with a variety of Southern Company subsidiaries in the areas of finance, strategy, international business development and technology. Elected by the board of directors in July 2010, he became president of Southern Company in August 2010, and assumed the additional responsibilities of chairman and CEO in December 2010. Mr. Fanning is co-chair of the Electricity Subsector Coordinating Council, which serves as the principal liaison between the federal government and the electric power sector to protect the electric grid from threats that could impact national security, including cyber and physical terrorism as well as natural disasters. He also collaborates with the Tri-Sector Executive Working Group, which was formed by the electricity, finance, and communications sectors to enhance national and economic security by developing a cross-sector strategic framework to address existential threats, risk, and consequence management. His leadership in cybersecurity was recognized by the U.S. Senate with an appointment to the Cyberspace Solarium Commission, a group developing a protection strategy for the cyberspace interests of the United States. From 2012-2018, Mr. Fanning served on the board of directors of the Federal Reserve Bank of Atlanta and is a past chairman. He is also a past chairman of the Conference of Chairs of the Federal Reserve Banks and the Edison Electric Institute (EEI).

Ms. Vijaya Gadde

Legal, Public Policy, and Trust and Safety Lead
Twitter

Ms. Vijaya Gadde is Twitter's legal, public policy, and trust and safety lead. Prior to joining Twitter in 2011, Ms. Gadde was senior director, legal at Juniper Networks; previously, for nearly a decade she worked at Wilson Sonsini Goodrich & Rosati. Ms. Gadde serves on the Board of Trustees of NYU Law School and the Board of Directors of Mercy Corps, a global humanitarian aid and development organization, which partners with communities, corporations, and governments. Ms. Gadde is also a co-founder of #Angels, an investment collective focused on funding diverse and ambitious founders pursuing bold ideas.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Dr. Patrick Gallagher

Chancellor
University of Pittsburgh

Dr. Patrick Gallagher serves as the University of Pittsburgh's chancellor, directing one of the nation's premier public institutions for higher education and research. In this role, he oversees a community of more than 33,000 students at five distinct campuses and supports more than 14,000 faculty and staff members who are committed to advancing the University's legacy of academic excellence, community service and research innovation. Under Dr. Gallagher's leadership, Pitt has strengthened its status as one of the nation's premier public institutions for higher education and research, including being named a top public school in the nation by U.S. News & World Report. Prior to his installation as chancellor, Dr. Gallagher spent more than two decades in public service. In 2009, the president appointed him to direct the National Institute of Standards and Technology. While in this role, Dr. Gallagher also served as acting deputy secretary of commerce before leaving for Pitt in the summer of 2014.

Mr. Ron Green

Executive Vice President and Chief Security Officer (CSO)
Mastercard, Inc.

Mr. Ron Green is chief security officer for Mastercard, where he leads a global team that ensures the safety and security of the company's network, as well as internal and external products and services. He is responsible for corporate security, security architecture and engineering, cryptographic key management, business continuity, disaster recovery and emergency management. Mr. Green is a member of the company's Management Committee. He joined Mastercard in 2014 after serving as deputy chief information security officer at Fidelity Information Services (FIS). Prior to this position, he was director, Investigation and Protections Operations at Blackberry. Mr. Green also served as a senior vice president across several areas at Bank of America. He has extensive experience working with international and federal law enforcement agencies both as a special agent in the United States Secret Service and as an officer in the United States Army. With the Secret Service, Mr. Green worked protection and fraud investigations. He was one of the first agents to receive formal training on seizing and analyzing electronic evidence and worked on a number of international cyber-crime investigations. Mr. Green serves on the board of directors for SailPoint Technologies, chairs the Financial Services Sector Coordinating Council (FSSCC), and is a member of the U.S. Secret Service, Cyber Investigation Advisory Board.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Ms. Niloofar Razi Howe

Senior Operating Partner
Energy Impact Partners

Ms. Niloofar Razi Howe is currently a senior operating partner at Energy Impact Partners, a venture capital fund investing in companies shaping the energy landscape of the future. She also serves on the boards of directors of Tenable, Inc., Morgan Stanley Banks, Pondurance (as Executive Chair), Recorded Future, Swimlane, and Tamr. She is a life member at the Council on Foreign Relations and a Fellow, International Security Initiative, at New America, a nonprofit, nonpartisan think tank. Previously, Ms. Howe served as chief strategy officer and senior vice president of Strategy and Operations at RSA, a global cybersecurity company, where she led corporate strategy, corporate development and planning, business development, global program management, business operations, security operations and federal business development. Prior to RSA, Ms. Howe served as the chief strategy officer of Endgame (acquired by Elastic), a leading enterprise software security company, where she was responsible for driving market and product strategy, as well as leading marketing, product management, corporate development, and planning. Ms. Howe spent twelve years leading deal teams in private equity and venture capital; first as a principal at Zone Ventures, an early-stage venture capital firm in Los Angeles, and then as managing director at Paladin Capital Group, a Washington, D.C.-based private equity fund focused on investing in next-generation security companies.

Mr. Kevin Mandia

CEO
Mandiant

Mr. Kevin Mandia is the Chief Executive Officer and a Director of Mandiant, formerly FireEye. Mr. Mandia was appointed FireEye CEO in June 2016 and joined the company's Board of Directors in February 2016. He was previously President of FireEye from February 2015 until June 2016. Mr. Mandia joined FireEye as Senior Vice President and Chief Operating Officer in December 2013, when FireEye acquired Mandiant, the company he founded in 2004. Before Mandiant, Mr. Mandia was the Director of Computer Forensics at Foundstone (acquired by McAfee Corporation) from 2000 to 2003, and the Director of Information Security for Sytex (later acquired by Lockheed Martin) from 1998 to 2000. Mr. Mandia also served in the United States Air Force, where he was a computer security officer in the 7th Communications Group at the Pentagon, and a special agent in the Air Force Office of Special Investigations (AFOSI).

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Mr. Jeff Moss

President
DEF CON Communications

Mr. Jeff Moss is the founder and President of DEF CON Communications, which organizes and manages the annual DEF CON information security conference. He is an internationally recognized expert in internet and information security. Since 2017, Mr. Moss has also served as a commissioner on the Global Council on the Stability of Cyberspace (GCSC). In 2016, Mr. Moss joined Richemont as a Director and a member of the Board's Nominations and Strategic Security Committees. Between April 2011 and December 2013 Mr. Moss was the Chief Security Officer and for the Internet Corporation for Assigned Names and Numbers. Prior to creating Black Hat Briefings, Mr. Moss was a director at Secure Computing Corporation where he helped establish their Professional Services Department. He started his professional career at Ernst & Young, LLP in their Information System Security division. In 2013 Mr. Moss was appointed as a Nonresident Senior Fellow at the Atlantic Council, associated with the Cyber Statecraft Initiative, within the Brent Scowcroft Center on International Security. From 2009 through 2020 Mr. Moss was a member of the U.S. Department of Homeland Security Advisory Council.

Ms. Nuala O'Connor

Senior Vice President & Chief Counsel, Digital Citizenship
Walmart

Ms. Nuala O'Connor is the Senior Vice President and Chief Counsel, Digital Citizenship at Walmart. She oversees the Digital Citizenship team responsible for providing advice across the company on issues related to privacy, use of data and data governance, use of emerging technologies, cybersecurity, and records management. Ms. O'Connor is a member of the President's Inclusion Council, which focuses on advising, collaborating, and inspiring on issues and enterprise efforts to promote inclusive environments. Before joining Walmart, she served as the President and CEO of the Center for Democracy and Technology, a global nonprofit focused on digital civil liberties. In the private sector, Ms. O'Connor served as both Vice President of Compliance and Customer Trust and Associate General Counsel for Privacy and Data Protection at Amazon, was the Chief Privacy Leader at General Electric, and held both privacy leadership and legal counsel roles at DoubleClick. In the public sector, Ms. O'Connor served as the first Chief Privacy Officer at the U.S. Department of Homeland Security (DHS) where she founded the DHS privacy office and was responsible for groundbreaking policy development on the use and protection of personal information in national security and law enforcement settings. She also previously served as deputy director of the Office of Policy and Strategic Planning, and later as Chief Counsel for Technology at the U.S. Department of Commerce.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Ms. Nicole Perlroth

Author and Journalist

Ms. Nicole Perlroth spent a decade at The New York Times where she was the lead reporter on cybersecurity and digital espionage. Over her career she has reported on Russian hacks of nuclear plants, petrochemical plants, and elections; North Korea's cyberattacks against movie studios, banks and hospitals; Iranian attacks on oil companies, banks and political campaigns; and hundreds of Chinese cyberattacks, including a months-long hack of The New York Times. She is the author of the New York Times bestselling book "This Is How They Tell Me the World Ends," about the global cyber arms race. Ms. Perlroth is the recipient of several journalism awards including best technology reporting by the Society of Business Editors and Writers.

Mr. Matthew Prince

Chief Executive Officer
Cloudflare

Mr. Matthew Prince is co-founder and CEO of Cloudflare, a web infrastructure and security company. Today the company runs one of the world's largest networks, which spans more than 250 cities in over 100 countries, and is recognized by Inc. Magazine as one of the Best-Led Companies in America. Mr. Prince is a World Economic Forum Technology Pioneer, a permanent member of the Council on Foreign Relations, and a winner of the 2011 Tech Fellow Award. Prior to founding Cloudflare, he co-created Project Honey Pot, an open-source community of webmasters that monitors online fraud and abuse.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Mr. Stephen Schmidt

Chief Information Security Officer
Amazon Web Services

Mr. Stephen Schmidt is Vice President and Chief Information Security Officer for Amazon Web Services (AWS). His duties at AWS include leading product design, management and engineering development efforts focused on bringing the competitive, economic and security benefits of cloud computing to business and government customers. Prior to joining AWS, Mr. Schmidt had an extensive career at the Federal Bureau of Investigation, where he served as a senior executive. His responsibilities at the FBI included a term as acting Chief Technology Officer, Section Chief responsible for the FBI's technical collection and analysis platforms, and as a Section Chief overseeing the FBI's Cyber Division components responsible for the technical analysis of computer and network intrusion activities.

Mr. Ted Schlein

General Partner
Kleiner, Perkins, Caufield, & Byers (KPCB)

Mr. Ted Schlein is a General Partner at Kleiner Perkins and a leading expert on cybersecurity and enterprise software. The founding Chief Executive Officer of Fortify Software, Mr. Schlein has led Kleiner Perkins' involvement in several successful investments including Alien Vault, Arcsight, CarbonBlack, Chegg, Internet Security Systems, IronNet, Phantom Security, Mandiant, Oakley Networks, Segment and Shape Security. Ted serves on the board of directors of several companies including Apiiro, Area1 Security, Chegg, FullStory, Interos, Incorta, Inspirato, IronNet, Rebellion Defense, Reputation, Synack, Trusona and UJet. Prior to Kleiner Perkins, Mr. Schlein served as Vice President, Enterprise Solutions at Symantec and led Symantec's move into the software utilities market, launching its commercial antivirus solution that quickly emerged as the industry gold standard. Mr. Schlein is the former chairman of the National Venture Capital Association (NVCA), the former president of the Western Association of Venture Capitalist and is the founder of DoD-sponsored DeVenCI program. He currently serves on the Board of Trustees of the University of Pennsylvania and the Dean's Board of Advisors of the Engineering School at the University of Pennsylvania. Additionally, Ted serves on the Board of Trustees at InQTel and frequently participates as an opinion leader in public, private and government forums, providing perspectives on security technology, related investments, and market adoption trends.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Ms. Suzanne Spaulding

Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions
Center for Strategic and International Studies

Ms. Suzanne Spaulding is senior adviser for homeland security and director of the Defending Democratic Institutions project at the Center for Strategic and International Studies (CSIS). She also serves as a member of the Cyberspace Solarium Commission. Previously, Ms. Spaulding served as Under Secretary for National Protection and Programs at the Department of Homeland Security (DHS), charged with strengthening cybersecurity and protecting the nation's critical infrastructure. In this role she led the development and implementation of national policies for strengthening the security and resilience of critical infrastructure against cyber and physical risks, including the National Infrastructure Protection Plan and key presidential directives and executive orders. Ms. Spaulding also led security regulation of the chemical industry, biometrics and identity management, emergency communications, and the Federal Protective Service. As a member of the board of directors for the First Responder Network Authority, Ms. Spaulding helped oversee the complex and unprecedented effort to deploy the first nation-wide broadband network for public safety. Outside of her government roles, Ms. Spaulding has worked in the private sector, including as Security Counsel for the Business Roundtable, and currently serves on a number of corporate and non-profit boards.

Mr. Alex Stamos

Partner
Krebs Stamos Group

Mr. Alex Stamos is working to improve the security and safety of the Internet through teaching and research as the Director of the Stanford Internet Observatory, a cross-disciplinary program studying the abuse of the internet. He also helps companies secure themselves as a Partner in the Krebs Stamos Group. He has served as Chief Security Officer at Facebook and Yahoo and was a co-founder of iSEC Partners. Mr. Stamos has investigated and responded to several historical events and has been called the "Forrest Gump of InfoSec" by friends. He is a member of the Aspen Cybersecurity and Information Disorder Commissions, Annan Commission on Elections and Democracy and advises NATO's Cybersecurity Center of Excellence. He has spoken on six continents, testified in Congress, served as an expert witness for the wrongly accused, and holds five patents.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Mr. Georgios Stathakopoulos

Vice President of Corporate Information Security
Apple

Mr. Georgios Stathakopoulos leads the Enterprise information security program at Apple, which protect Apple's corporate assets, retail stores, and customer data. Prior to joining Apple, Mr. Stathakopoulos served as Vice President of Information Security and Corporate IT at Amazon. George's organization built programs to protect Amazon and its customers, and was also responsible for IT infrastructure and other technology resources. He began his career in information security at Microsoft, where he served as General Manager of the Microsoft Security Response Center, responsible for product security. Originally from Athens, Greece, Mr. Stathakopoulos holds a BA in Computer Science from Portland State University.

Dr. Kate Starbird

Associate Professor, Human Centered Design & Engineering
University of Washington

Dr. Kate Starbird is an Associate Professor in the Department of Human Centered Design & Engineering and is a co-founder and current Faculty Director of the Center for an Informed Public at the University of Washington. She is also adjunct faculty at the Paul G. Allen School of Computer Science & Engineering and a data science fellow at the eScience Institute. Dr. Starbird's research addresses human-computer interaction and the emerging field of crisis informatics — the study of how information and communication technologies are used during crisis events. Her research examines how people use social media to seek, share, and make sense of information after natural disasters (such as earthquakes and hurricanes) and man-made crisis events (such as acts of terrorism and mass shooting events). Her current focus is on the spread of disinformation in this context. Dr. Starbird's research touches on broader questions about the intersection of technology and society—including the vast potential for online social platforms to empower people to work together to solve problems, as well as salient concerns related to abuse and manipulation of and through these platforms and the consequent erosion of trust in information.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Ms. Alicia Tate-Nadeau

Illinois Homeland Security Advisor and Director
Illinois Emergency Management Agency

Ms. Alicia Tate-Nadeau was appointed by Governor J.B. Pritzker to serve as the Illinois Homeland Security Advisor and Director of the Illinois Emergency Management Agency (IEMA) in January 2019. Ms. Tate-Nadeau brings more than three decades of experience in national security, emergency management, and public safety issues. Prior to her appointment to Director of IEMA, Ms. Tate-Nadeau served as Executive Director of the Chicago Office of Emergency Management and Communications where she implemented and managed the third largest 9-1-1 call center in the nation. Ms. Tate-Nadeau spent more than three decades with the Illinois National Guard, retiring in 2017. Her time in the military included serving as the Assistant Adjutant General for the Illinois National Guard and concurrently as the Deputy Commanding General, Army National Guard, United States Army Maneuver Support Center of Excellence in Fort Leonard Wood, Missouri.

Ms. Nicole Wong

Principal
NWong Strategies Group

Ms. Nicole Wong is the Principal of NWong Strategies, where she specializes in assisting high-growth technology companies and non-profit organizations to develop international privacy, content, and regulatory strategies. She previously served as Deputy U.S. Chief Technology Officer in the Obama Administration, focused on internet, privacy, and innovation policy. Prior to her time in government, Ms. Wong was Google's Vice President and Deputy General Counsel, and Twitter's Legal Director for Products. She is an internationally recognized expert on privacy and free expression, and frequently speaks on issues related to law and technology, including five appearances before the U.S. Congress. Ms. Wong serves on the boards of the Filecoin Foundation, an independent organization that stewards the growth of technologies for a decentralized web; Friends of Global Voices, a non-profit organization dedicated to supporting citizen and online media projects globally; The Markup, a non-profit investigative news organization covering technology; and the Mozilla Foundation, which promotes the open internet. She also currently serves as an advisor to the AI Now Institute, the Albright Stonebridge Group, the Alliance for Securing Democracy, the Center for New American Security's Digital Freedom Forum, Luminate, Refactor Capital, and WITNESS.

CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MEMBER BIOGRAPHIES

Mr. Christopher Young

Executive Vice President, Business Development, Strategy, and Ventures
Microsoft

Mr. Christopher Young is Executive Vice President of business development, strategy, and ventures at Microsoft. He is responsible for driving growth across the company by establishing strategic partnerships, setting corporate strategy, and identifying high impact investments through Microsoft's corporate venture arm. Mr. Young is the former CEO of McAfee, LLC. Under his leadership, McAfee grew to protect mission-critical systems and data for more than two-thirds of the Global 2000 and more than 500 million consumers. Earlier in his career, Mr. Young led cybersecurity efforts at Cisco, RSA and AOL. He also led end user computing at VMware and cofounded the company Cyveillance. Mr. Young currently serves on the board of directors of American Express. He previously served as a member of the President's National Security Telecommunications Advisory Committee. He has also been a board member of Snap Inc., Rapid7, and the Cyber Threat Alliance, and has served on the board of trustees of Princeton University.

9110-9P

DEPARTMENT OF HOMELAND SECURITY

Cybersecurity and Infrastructure Security Agency

Docket No. CISA-2021-0017

Notice of Cybersecurity and Infrastructure Security Agency Cybersecurity Advisory Committee Meeting

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: Notice of *Federal Advisory Committee Act* (FACA) meeting; request for comments.

SUMMARY: CISA is publishing this notice to announce the following CISA Cybersecurity Advisory Committee meeting. This meeting will be partially closed to the public.

DATES: *Meeting Registration:* Registration to attend the meeting is required and must be received no later than 5:00 p.m. Eastern Time (ET) on December 8, 2021. For more information on how to participate, please contact CISA CybersecurityAdvisoryCommittee@cisa.dhs.gov.

Speaker Registration: Registration to speak during the meeting's public comment period must be received no later than 5:00 p.m. ET on December 8, 2021.

Written Comments: Written comments must be received no later than 5:00 p.m. ET on December 8, 2021.

Meeting Date: The CISA Cybersecurity Advisory Committee will meet on December 10, 2021, from 10:30 a.m. to 3:30 p.m. ET. The meeting may close early if the committee has completed its business.

ADDRESSES: The CISA Cybersecurity Advisory Committee's open session will be held in-person at 7525 Colshire Drive, McLean, VA 22102. Capacity and location are subject to change based on DHS protocol regarding COVID-19 pandemic restrictions at the time of the meeting. Due to pandemic restrictions, members of the public may participate via teleconference only. Requests to participate will be accepted and processed in the order in which they are received. For access to the conference call bridge, information on services for individuals with disabilities, or to request special assistance, please email CISA CybersecurityAdvisoryCommittee@cisa.dhs.gov. by 5:00 p.m. ET on December 8, 2021.

Comments: Members of the public are invited to provide comments on issues that will be considered by the committee as outlined in the **SUPPLEMENTARY INFORMATION** section below. Associated materials that may be discussed during the meeting will be made available for review at https://www.cisa.gov/cisa-cybersecurity-advisory-committee on November 24, 2021. Comments should be submitted by 5:00

p.m. ET on December 10, 2021, and must be identified by Docket Number CISA-2021-0017. Comments may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** www.regulations.gov. Please follow the instructions for submitting written comments.
- **Email:** CISA CybersecurityAdvisoryCommittee@cisa.dhs.gov. Include the Docket Number CISA-2021-0017 in the subject line of the email.

Instructions: All submissions received must include the words "Department of Homeland Security" and the Docket Number for this action. Comments received will be posted without alteration to www.regulations.gov, including any personal information provided.

Docket: For access to the docket and comments received by the CISA Cybersecurity Advisory Committee, please go to www.regulations.gov and enter docket number CISA-2021-0017.

A public comment period is scheduled to be held during the meeting from 3:10 p.m. to 3:20 p.m. ET. Speakers who wish to participate in the public comment period must email CISA CybersecurityAdvisoryCommittee@cisa.dhs.gov to register. Speakers should limit their comments to 3 minutes and will speak in order of registration. Please note that

the public comment period may end before the time indicated, depending on the number of speakers who register to participate.

FOR FURTHER INFORMATION CONTACT: Megan Tsuyi, [redacted], CISA CybersecurityAdvisoryCommittee@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: The CISA Cybersecurity Advisory Committee was established under the National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283). Notice of this meeting is given under FACA, 5 U.S.C. Appendix (Pub. L. 92-463). The CISA Cybersecurity Advisory Committee advises the CISA Director on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

Agenda: The CISA Cybersecurity Advisory Committee will meet in an open session on Friday, December 10, 2021, from 1:00 p.m. to 3:30 p.m. ET to discuss CISA Cybersecurity Advisory Committee activities and the Government's ongoing cybersecurity initiatives. The open session will include: (1) a keynote address; (2) an overview of CISA; and (3) a discussion on CISA's big challenges, priorities, and potential study topics for the CISA Cybersecurity Advisory Committee.

The committee will also meet in a closed session from 10:30 a.m. to 12:00 p.m. ET during which time senior Government intelligence officials will provide a classified threat briefing concerning cybersecurity threats to the Government and critical infrastructure.

Basis for Closure: In accordance with section 10(d) of FACA and 5 U.S.C. 552b(c)(1), *The Government in the Sunshine Act*, it has been determined that one agenda item requires closure, as the disclosure of the information that will be discussed would not be in the public interest.

This agenda item includes a threat briefing, which will provide CISA Cybersecurity Advisory Committee members the opportunity to discuss information concerning cybersecurity threats with senior Government intelligence officials. The briefing is anticipated to be classified at the top secret/sensitive compartmented information level. Disclosure of the threats, vulnerabilities, and mitigation techniques discussed during the briefing would present a risk to the Nation's cybersecurity posture, as adversaries could use this information to compromise commercial and Government networks. The premature disclosure of this information to the public would provide adversaries who wish to intrude into commercial and government networks with information on potential vulnerabilities, current

mitigation techniques, and existing cybersecurity defense tactics.

Therefore, this portion of the meeting is required to be closed pursuant to section 10(d) of FACA and 5 U.S.C. 552b(c)(1), (3).

Megan Tsuyi
Designated Federal Officer, CISA Cybersecurity Advisory Committee
Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY CYBERSECURITY ADVISORY COMMITTEE CHARTER

1. Committee's Official Designation:

Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee

2. Authority:

CISA [hereinafter referred to as the "Agency"] Cybersecurity Advisory Committee is established under the *National Defense Authorization Act* for Fiscal Year 2021, P.L. 116-283 (NDAA). Pursuant to section 871(a) of the *Homeland Security Act of 2002*, 6 U.S.C. § 451(a), the Secretary of Homeland Security hereby establishes the CISA Cybersecurity Advisory Committee for the purposes set forth herein. This Committee is established in accordance with and operates under the provisions of the *Federal Advisory Committee Act* (FACA) (Title 5, United States Code, Appendix).

3. Objectives and Scope of Activities

The CISA Cybersecurity Advisory Committee shall develop, at the request of the CISA Director [hereinafter referred to as the "Director"] and incorporating guidance where applicable from the Secretary of Homeland Security [hereinafter referred to as the "Secretary"], recommendations on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

4. Description of Duties

The duties of the CISA Cybersecurity Advisory Committee are solely advisory in nature, as established under the *National Defense Authorization Act* for Fiscal Year 2021, P.L. 116-283 (NDAA). Pursuant to section 871(a) of the *Homeland Security Act of 2002*, 6 U.S.C. § 451(a). The CISA Cybersecurity Advisory Committee shall also submit to the Director, with a copy to the Secretary, an annual report providing information on the activities, findings, and recommendations of the Committee, including its subcommittees, for the preceding year.

5. Officials to Whom the Committee Reports

The CISA Cybersecurity Advisory Committee will advise, consult with, report to, and make independent, strategic, and actionable recommendations to the CISA Director.

6. Agency Responsible for Providing Necessary Support:

CISA shall be responsible for providing financial and administrative support to the CISA Cybersecurity Advisory Committee.

7. Estimated Cost, Compensation, and Staff Support:

The estimated annual cost of operating the CISA Cybersecurity Advisory Committee is approximately $1,450,000, which includes travel and per diem, and other administrative expenses, and five Full-Time Equivalent employees to support the Committee.

8. Designated Federal Officer:

The Director shall appoint full-time employees of the Agency as the Designated Federal Officer (DFO) and Alternate DFOs (ADFO). The DFO or the ADFO will be responsible for setting agendas and the Committee's work activities. The DFO or the ADFO will coordinate with the Homeland Security Advisory Council's DFO [hereinafter referred to as the "HSAC"] to minimize duplication and ensure complementary work activities between both groups. The DFO or ADFO approves or calls the CISA Cybersecurity Advisory Committee and subcommittee meetings, attends all committee and subcommittee meetings, adjourns any meetings when it is determined adjournment to be in the public interest, and chairs the meeting in the absence of the designated CISA Cybersecurity Advisory Committee Chair.

9. Estimated Number and Frequency of Meetings:

CISA Cybersecurity Advisory Committee meetings will be held semiannually, at a minimum, to address matters within the scope of this Charter. Meetings may be held more frequently, or as necessary and appropriate, to address mission requirements. Meetings shall be open to the public according to the FACA unless a determination is made by the appropriate DHS official in accordance with DHS policy and directives that the meeting should be closed in accordance with Title 5, United States Code, subsection (c) of 552b. At least one meeting per year will be open to the public.

10. Duration

Continuing.

11. Termination

This charter shall be in effect for two years from the date it is filed with Congress unless sooner terminated. The charter may be renewed at the end of this two year period in accordance with section 14 of FACA (5 U.S.C. App.).

12. Membership and Designation

The Committee shall be composed of up to 35 individuals. Members are appointed by the Director. The DFO will coordinate with the DFO for the HSAC to ensure that

individuals selected for appointment to the Committee are not presently or under consideration to be members of the HSAC.

In order for the Director to fully leverage broad-ranging experience and education, the CISA Cybersecurity Advisory Committee must be diverse, with regard to professional and technical expertise, and in reflecting the diversity of the nation's people. These members shall consist of subject matter experts from diverse and appropriate professions and communities nationwide, be geographically balanced, and shall include representatives of State, local, tribal, and territorial governments and of a broad and inclusive range of industries. The CISA Director may, at their discretion, select members with a background in cybersecurity issues relevant to CISA policies, plans, and programs. Specifically, membership may, at the CISA Director's discretion, include at least one, and no more than three, representatives from the following industries recommended in the authorizing statute:

i. Defense;

ii. Education;

iii. Financial services and insurance;

iv. Healthcare;

v. Manufacturing;

vi. Media and entertainment;

vii. Chemical;

viii. Retail;

ix. Transportation;

x. Energy;

xi. Information Technology;

xii. Communications; and

xiii. Other relevant fields identified by the Director.

The term of each member shall be two years, except that a member may continue to serve until a successor is appointed. Appointments are personal to the member and cannot be transferred to another individual or other employees of the member's organization of employment. A member may be reappointed for an unlimited number of terms. The Director may review the participation of a member of the CISA Cybersecurity Advisory Committee and remove such member any time at his/her discretion to include for violation of established responsibilities as outlined in sections III.6 and III.7 of the committee's bylaws.

Members shall serve as representatives to speak on behalf of their respective organizations

Members of the CISA Cybersecurity Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the CISA Cybersecurity Advisory Committee.

13. Officers

The CISA Cybersecurity Advisory Committee shall select a Chair and Vice Chair from among its members through a nomination and formal vote. The Chair and Vice Chair will serve for a two-year term. The CISA Cybersecurity Advisory Committee Chair shall preside at all CISA Cybersecurity Advisory Committee meetings, unless chaired by the Vice Chair, DFO, or ADFO. In the Chair's absence, the Vice Chair will act as the Chair. Additionally, the CISA Cybersecurity Advisory Committee shall select a member to serve as chairperson of each subcommittee.

14. Subcommittees

The Director, through the DFO, establishes subcommittees for any purpose consistent with this charter. The DFO will coordinate with the HSAC DFO to ensure that subcomittees are established in such a manner as to minimize duplication and ensure complementary work activities between both groups.

The CISA Cybersecurity Advisory Committee Chair shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee. Such subcommittees may not work independently of the chartered committee and must present their advice or work products to the CISA Cybersecurity Advisory Committee for full deliberation and discussion.

Each subcommittee shall meet semiannually, at a minimum, and submit to the CISA Cybersecurity Advisory Committee for inclusion in the annual report, activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

Subcommittees have no authority to make decisions on behalf of the CISA Cybersecurity Advisory Committee and may not report directly to the Federal Government or any other entity.

15. Recordkeeping:

The records of the CISA Cybersecurity Advisory Committee, formally and informally established subcommittees, or other subgroups of the Committee shall be handled in accordance with General Records Schedule 6.2, or other applicable and approved agency records disposition schedule. These records shall be available for public

inspection and copying in accordance with the Freedom of Information Act (Title 5, United States Code, section 552).

16. Filing Date:

May 21, 2021

Department Approval Date

May 24, 2021

GSA Consultation Date

June 25, 2021

Date Filed with Congress

September 3, 2021

Date Amendment Filed with Congress

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
CYBERSECURITY ADVISORY COMMITTEE
BYLAWS

I. AUTHORITY

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee is established under the *National Defense Authorization Act* for Fiscal Year 2021, P.L. 116-283 (NDAA). Pursuant to section 871(a) of the *Homeland Security Act of 2002*, 6 U.S.C. § 451(a), the Secretary of Homeland Security hereby establishes the CISA Cybersecurity Advisory Committee for the purposes set forth herein. This statutory committee is established in accordance with and operates under the provisions of the *Federal Advisory Committee Act* (FACA) (Title 5, United States Code, Appendix).

II. PURPOSE

The CISA Cybersecurity Advisory Committee will provide independent, strategic, and actionable consensus recommendations to CISA on a range of cybersecurity issues, topics, and challenges, including, but not limited to: information exchange; critical infrastructure; risk management; and public and private partnerships. The CISA Cybersecurity Advisory Committee shall develop, at the request of the CISA Director [hereinafter referred to as the "Director"], and incorporating guidance from the Secretary of Homeland Security [hereinafter referred to as the "Secretary"], recommendations on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

III. MEMBERSHIP AND MEMBER RESPONSIBILITIES

1. *Composition*

The Committee shall be composed of up to 35 members. Members are appointed by the Director. The CISA Cybersecurity Advisory Committee Designated Federal Officer (DFO) will coordinate with the DFO for the Homeland Security Advisory Council (HSAC) to ensure that individuals selected for appointment to the Committee are not presently or under consideration to be members of the HSAC. In order for the Director to fully leverage broad-ranging experience and education, the CISA Cybersecurity Advisory Committee must be diverse, with regard to professional and technical expertise, and in reflecting the diversity of the nation's people. These members shall consist of subject matter experts from diverse and appropriate professions and communities nationwide, be geographically balanced, and include representatives from State, local, tribal, and territorial governments and a broad and inclusive range of industries. The Director may, at their discretion, select members with a background in cybersecurity issues relevant to CISA policies, plans, and programs. Specifically, membership may, at

the Director's discretion, include at least one, and no more than three, representatives from the following industries recommended in the authorizing statute:

i. Defense;

ii. Education;

iii. Financial services and insurance;

iv. Healthcare;

v. Manufacturing;

vi. Media and entertainment;

vii. Chemical;

viii. Retail;

ix. Transportation;

x. Energy;

xi. Information Technology;

xii. Communications; and

xiii. Other relevant fields identified by the Director.

Members shall serve as representatives to speak on behalf of their respective organizations.

2. *Appointment*

Members of the Committee are appointed by and serve at the pleasure of the Director. Membership is voluntary and members are not compensated for their services. Appointments are personal to the member and cannot be transferred to another individual or other employees of the member's organization of employment. Members may not designate someone to attend in their stead, participate in discussions, or vote. If a member becomes a federal employee or otherwise ineligible for membership, the member must inform the CISA Cybersecurity Advisory Committee DFO. Additionally, if it is the intent of the member to resign, he or she must submit the request in writing to the Director as well as the DFO.

3. *Terms of Office*

   Members will serve two-year staggered terms. A member may be reappointed for an unlimited number of terms. In the event that the CISA Cybersecurity Advisory Committee terminates, all appointments to the Committee shall terminate.

4. *Certification of Non-Lobbyist Status*

   Members of the CISA Cybersecurity Advisory Committee who serve as representatives of an association or organization shall register as required in accordance with the requirements of the *Lobbying Disclosure Act* if they engage in lobbying activities or are a lobbying contact as defined in 2 U.S.C. 1602. Any individual who so registers shall advise the DFO of such registration within 30 days of the registration or prior to the first meeting of the CISA Cybersecurity Advisory Committee, whichever occurs first.

5. *Security Clearances*

   Members are not required to have security clearances to participate in committee activities.

6. *Members' Responsibilities*

   Since the membership of the CISA Cybersecurity Advisory Committee is constructed to balance as many aspects and viewpoints as possible, member attendance and participation at meetings is vital to the CISA Cybersecurity Advisory Committee's mission. Members are expected to personally attend and participate in Committee meetings and conference calls. The Director may review the participation of a member of the CISA Cybersecurity Advisory Committee and remove such member any time at the discretion of the Director. The DFO will recommend to the Director that any member who is unable to fulfill his/her responsibility be removed from the Committee. Members of the CISA Cybersecurity Advisory Committee may be recommended for removal by the DFO for reasons such as, but not limited to:

   a. Missing two consecutive meetings, or not participating in the Committee's work; and
   b. Engaging in activities that are illegal or violate the restrictions on members' activities as outlined below.

7. *Restriction on Members' Activities*

   a. Members may not use their access to the Federal Government as a member of this Committee for the purpose of soliciting business for or otherwise seeking economic advantage for themselves, their companies, or their employers. Members may not use any non-public information obtained in the course of their duties as a

member for personal gain or for that of their company or employer. Members must hold any non-public information, including pre-decisional documents such as draft reports, in confidence.

b. The Committee as a whole may advise CISA on legislation or may recommend legislative action to CISA. In their capacities as members of the CISA Cybersecurity Advisory Committee, individual members may not petition or lobby Congress for or against particular legislation or encourage others to do so.
c. Subcommittees of the Committee may only advise CISA on legislation or policy with the approval and authorization of the full Committee membership.
d. Members of the CISA Cybersecurity Advisory Committee are advisors to the agency and have no authority to speak for the Committee, CISA, or for the Department of Homeland Security (DHS) outside of the Committee structure.
e. Members may not testify before Congress in their capacity as a member of the CISA Cybersecurity Advisory Committee. If requested to testify before Congress, members of the CISA Cybersecurity Advisory Committee:
    i. Cannot represent or speak for the Committee, CISA, DHS, or any agency or the Administration in their testimony.
    ii. Cannot provide information or comment on Committee recommendations that are not publicly available.
    iii. May state that they are a member of the Committee.
    iv. May speak to their personal observations as to their service on the Committee.
f. If speaking outside of the Committee structure at other forums or meetings, the restrictions in Section (d) also apply.

IV. OFFICIALS

1. *CISA Cybersecurity Advisory Committee Leadership*

The CISA Cybersecurity Advisory Committee will select a Chair and Vice Chair from among the Committee members through a nomination and formal vote. The Chair and Vice Chair will serve for a two-year term. The Chair and/or Vice Chair may be reappointed for additional terms, not to exceed two terms. The DFO may determine that the Chair or Vice Chair's term be extended by no more than six months, in order to complete their oversight of an outstanding task or report. If a Chair or Vice Chair is not able to serve for their entire term, an additional election will be held. The CISA Cybersecurity Advisory Committee Chair will preside at all CISA Cybersecurity Advisory Committee meetings. The Chair will conduct the meeting, provide an opportunity for participation by each member and by public attendees, ensure adherence to the agenda, maintain order, and prepare any recommendations submitted to the Agency. The Vice Chair will act as the Chair in the absence of the Chair. The Chair and Vice Chair are expected to facilitate

Committee meetings and moderate all Committee deliberations. The Chair and Vice Chair will receive taskings from the Director and/or the DFO, in coordination with HSAC DFO, and in coordination with the DFO, will create subcommittees to examine taskings.

2. *Designated Federal Officer*

The DFO and the Alternate DFO (ADFO) serve as CISA's agent for all matters related to the CISA Cybersecurity Advisory Committee and are appointed by the Director. The DFO or ADFO will:

a. Approve agendas for Committee and subcommittee meetings;
b. Attend all meetings of the CISA Cybersecurity Advisory Committee to ensure the advisory activities of the Committee are within its authorized scope of responsibility;
c. Approve or call meetings of the Committee and subcommittees;
d. Adjourn meetings when such adjournment is in the public interest;
e. Chair meetings of the Committee when directed to do so by the Director or when requested in the absence of the Chair; and
f. Assist the Director in his/her reporting requirements, as outlined in Section X. This may include ensuring final Committee reports are posted on the CISA Cybersecurity Advisory Committee's publicly available website and assisting with the preparation for the Director's annual briefing to Congress.

Additionally, the DFO is responsible for assuring administrative support functions are performed, including:

a. Notifying members and for open meetings, the general public, of the time and place of each meeting;
b. Tracking all recommendations of the Committee;
c. Maintaining the record of members' attendance;
d. Preparing the minutes of all meetings of the Committee's deliberations;
e. Releasing minutes and agendas of all meetings to the general public in the manner required by law unless a specific meeting is closed to the public;
f. Attending to official correspondence;
g. Maintaining official records and filing all papers and submissions prepared for or by the Committee;
h. Developing or updating operating procedures for all Committee activities;
i. Reviewing and updating information on Committee activities in the FACA database on a monthly basis;
j. Acting as the Committee's agent to collect, validate, and pay for all vouchers for pre-approved expenditures; and
k. Preparing and handling all reports.

V. MEETING PROCEDURES

1. *Meeting Schedule and Call of Meetings*

   The CISA Cybersecurity Advisory Committee will meet at least twice per year to address matters within the scope of the Committee's charter. Meetings may be held more frequently, or as necessary and appropriate, to address mission requirements. Additional meetings may be scheduled, pending approval from the DFO or ADFO. The DFO or ADFO must attend all Committee meetings.

2. *Agenda*

   Meeting agendas are developed by the DFO and CISA staff in coordination with the CISA Cybersecurity Advisory Committee Chair. The DFO will approve the agenda for all Committee meetings and approve the agenda for subcommittee meetings, distribute the agenda to members prior to the meeting, and, in the event of a public meeting, will publish the agenda for Committee meetings in the Federal Register.

3. *Quorum*

   A quorum of CISA Cybersecurity Advisory Committee members is the presence of fifty percent plus one of the Committee members currently appointed. A quorum of the Committee is required to vote on issues being addressed. In the event a quorum is not present, the CISA Cybersecurity Advisory Committee may conduct business that does not require a vote or decision among members. Votes will be deferred until such a time that a quorum is present.

4. *Voting Procedures*

   Members will review recommendations and reports from the CISA Cybersecurity Advisory Committee subcommittees and working groups. Any item being presented to the Committee for approval must be made available to the public in advance of a Committee meeting, must be discussed by the Committee during the meeting, and must receive a majority vote from the Committee, unless the Committee is meeting in closed session pursuant to procedures set forth in law. When a decision or recommendation of the CISA Cybersecurity Advisory Committee is required, the Chair will request a motion for a vote. A motion is considered to have been adopted if agreed to by a simple majority of a quorum of CISA Cybersecurity Advisory Committee members. Only members present at the meeting may vote on an item under consideration. No proxy votes or votes by email will be allowed.

5. *Minutes*

   The DFO will prepare the minutes of each meeting and distribute copies to each Committee member. Minutes of open meetings will be available to the public on

the CISA Cybersecurity Advisory Committee website. The minutes will include a record of:

a. The time, date, and place of the meeting;
b. A list of all attendees, including Committee members, staff, agency employees, and members of the public who presented oral or written statements;
c. An accurate description of each matter discussed and the resolution, if any, made by the Committee; and
d. An accurate description of public participation, including oral and written statements provided.

Minutes of closed meetings will also be available to the public upon request, subject to the withholding of matters about which public disclosure would be harmful to the interests of the Government, industry, or others, and which are exempt from disclosure under the *Freedom of Information Act* (5 U.S.C., Section 552). The DFO ensures that the Chair certifies the minutes within 90 calendar days of the meeting to which they relate.

6. *Open Meetings*

The CISA Cybersecurity Advisory Committee is required to hold at least one public meeting per year. Unless otherwise determined in advance, all meetings of the CISA Cybersecurity Advisory Committee will be published in the Federal Register at least fifteen calendar days before the meeting. Members of the public may attend any meeting or portion of a meeting that is not closed to the public and may, at the determination of the DFO, offer oral comment at such meeting. Oral comments should be allowed unless it is clearly inappropriate to do so. Members of the public may submit written comments to the CISA Cybersecurity Advisory Committee. All materials provided to the committee shall be available to the public when they are provided to the members. Such materials, including any submissions by members of the public, are part of the meeting record.

7. *Closed Meetings*

Due to the sensitive nature of topics discussed, CISA Cybersecurity Advisory Committee meetings may be closed, or partially closed, in accordance with applicable law. A determination must be made by the CISA Director in accordance with DHS policy and directives that the meeting should be closed in accordance with Title 5, U.S.C., subsection (c) of section 552b. Where the DFO has determined in advance that discussion during a committee meeting will involve matters about which public disclosure would be harmful to the interests of the Government, industry, or others, an advance notice of a closed meeting, citing the applicable exemptions of the Government in the Sunshine Act, will be published in the Federal Register. The notice may announce the closing of all or part of a meeting. If, during the course of an open meeting, matters inappropriate for public disclosure arise during discussions, the DFO or the CISA Cybersecurity Advisory Committee Chair will order such discussion to cease and will schedule

it for a future committee meeting that will be approved for closure. No meeting or portion of a meeting may be closed without prior approval and notice published in the Federal Register at least 15 calendar days in advance. Closed meetings may only be attended by the DFO, Committee members, CISA and CISA Cybersecurity Advisory Committee staff, and appropriate Federal Government officials invited to provide subject matter expertise related to agenda items. Presenters must leave immediately after giving their presentations and answering any questions. Meetings may be opened by the CISA Cybersecurity Advisory Committee DFO or ADFO after consultation with participating leadership.

VI. EXPENSES AND REIMBURSEMENTS

CISA is responsible for providing financial and administrative support to the CISA Cybersecurity Advisory Committee. Members of the CISA Cybersecurity Advisory Committee will serve on the Committee without compensation. However, to the extent permitted by law, members may be reimbursed for travel and per diem expenses. Travel expenditures must be approved by the DFO in advance. CISA will be responsible for processing travel reimbursements for the CISA Cybersecurity Advisory Committee.

VII. ADMINISTRATION

CISA will provide administrative and clerical support to the Committee and assist in carrying out the administrative functions of the DFO as outlined in Article IV, Section 2.

VIII. SUBCOMMITTEES

The Director will establish subcommittees, as necessary. The DFO will coordinate with the HSAC DFO to ensure that subcomittees are established in such a manner as to minimize duplication and ensure complementary work activities between both groups. Subcommittee members may be composed in part or in whole of individuals who are not CISA Cybersecurity Advisory Committee members and are invited to serve the Committee by the CISA Cybersecurity Advisory Committee Chair. Subcommittees will be stood up as needed and terminate when the work is complete. The CISA Cybersecurity Advisory Committee members will consult with the DFO to determine the appropriate participants for each tasking.

1. *Subcommittee Leadership*

   CISA Cybersecurity Advisory Committee members shall select, from among the members of the Committee, a member to serve as chairperson of each subcommittee.

2. *Subcommittee Members*

   The CISA Cybersecurity Advisory Committee Chair shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee

has subject matter expertise relevant to the subject matter of the subcommittee. A subcommittee member's term of service will expire when the tasking is completed. Subcommittee members will reflect balanced viewpoints on the subject matter. All subcommittee discussions and materials, including briefings, outlines, and reports, are considered pre-decisional working drafts and shall not be publicly available. Once the tasking has been examined by a subcommittee, the subcommittee must present its work to the CISA Cybersecurity Advisory Committee for full deliberation and discussion.

3. *Meetings and Reporting*

Each subcommittee shall meet not less frequently than semi-annually. In addition to supporting taskings required by the Director, the subcommittee must also provide the CISA Cybersecurity Advisory Committee with information regarding its activities, findings, and recommendations for inclusion in the annual report.

IX. RECORDKEEPING

The DFO maintains all records of the CISA Cybersecurity Advisory Committee, formally or informally established subcommittees, or other subgroups in accordance with the General Records Schedule 6.2, or other approved agency, or CISA policies and procedures records disposition schedule. These records shall be available for public inspection and copying, in accordance with the *Freedom of Information Act* (Title 5, U.S.C., section 552). All documents, reports, or other materials presented to, or prepared by or for the Committee, constitute official government records and are available to the public upon request.

X. RECOMMENDATIONS AND REPORTING

The CISA Cybersecurity Advisory Committee shall submit to the Director reports on matters identified by the Director and reports on other matters identified by a majority of the Committee. The subcommittee assigned to a specific tasking will present the CISA Cybersecurity Advisory Committee with a draft report for the members to deliberate, discuss, and vote upon. Once the members agree on the final product, the product, in the form of a written report, will be transmitted to the Director within 14 days of the members approving it. Once received, the Director has 90 days to respond, in writing, to the Committee with feedback on the recommendations. If the Director concurs with the recommendation, the response should include an action plan to implement the recommendation. If the Director does not concur with a recommendation, the response should include a justification as to why the Director does not plan to implement the recommendation.

Additionally, the CISA Cybersecurity Advisory Committee shall submit to the Director, with a copy to the Secretary, an annual report providing information on the activities, findings, and recommendations of the CISA Cybersecurity Advisory Committee, including its subcommittees, for the preceding year. Not later than 180 days after the date on which the Director receives an annual report for a year, the

Director shall publish a public version of the report describing the activities of the CISA Cybersecurity Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5, United States Code. The Director will also be required to provide a briefing on feedback from the CISA Cybersecurity Advisory Committee to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives.

XI. BYLAWS APPROVAL AND AMENDMENTS

The DFO may amend these bylaws at any time, and the amendments shall become effective immediately.

Megan Tsuyi July 8, 2021

Megan Tsuyi
CISA Cybersecurity Advisory Committee Designated Federal Officer